15

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-335040

(43)Date of publication of application : 17.12.1996

(51)Int.Cl. G09C 1/00
H04H 1/00
H04H 1/02
H04L 9/00
H04L 9/10
H04L 9/12
H04N 7/167

(21)Application number : 07-159771

(22)Date of filing : 02.06.1995

(71)Applicant : FUJITSU LTD

(72)Inventor : AKIYAMA RYOTA
MUNAKATA AKIO
KOGA YUZURU
ISHIZAKI MASAYUKI
YOSHIOKA MAKOTO

(54) ENCIPHERING PROCESSING SYSTEM

(57)Abstract:

PURPOSE: To provide an enciphering processing system in which the frequent change of key is reduced by reinforcing the enciphering algorithmand the information transferring efficiency between a service provider and a service client can be improved.

CONSTITUTION: A random number generator 1 generates a first title key Ks1 and a second title key Ks2 on the basis of random numbers. A first DES enciphering circuit for title 6 enciphers the input information with the first title key Ks1. The initial value of the input information corresponds to the data identification ID and relative time information (PCR) extracted from the header of a packet. After the encipherment of the initial value was completedthe enciphered result of a second DES enciphering circuit for title 7 becomes the input information. The second DES enciphering circuit for title 7 enciphers the enciphered result value by the first DES enciphering circuit 6 with the second title key Ks2. An exclusive OR circuit 8 outputs the exclusive OR between the data stored in the packet and the enciphered result value of the second DES enciphering circuit 7. This forms the

enciphering data.

CLAIMS

[Claim(s)]

[Claim 1]Encryption mode of processing which enciphers said data delivered between a service provider which provides data and a service client which receives supply of data characterized by comprising the following.

A key generating means in which said service provider generates two keys based on a random number.

The 1st encoding means that enciphers data with two keys generated by this key generating means.

A data delivery means to deliver said data enciphered by this 1st encoding means to said service client.

The 2nd encoding means that enciphers said two keys with a master key of specified substance.

Have a key delivery means to deliver said two keys enciphered by this 2nd encoding means to said service clientand said service clientThe 1st decoding means that decrypts said two enciphered keys which were delivered by said key delivery means with a master key of said specified substance.

The 2nd decoding means that decrypts said enciphered data which was delivered by said data delivery means by said two keys decrypted by this 1st decoding means.

[Claim 2]Encryption mode of processing characterized by comprising the following in a service provider which delivers data stored in a packet to a service client.

A key generating means which generates the 1st key and 2nd key based on a random number.

The 1st enciphering circuit that enciphers input with said 1st key.

An extraction means to extract time information from a header of said packetand to input this time information into said 1st enciphering circuit as an initial value of said input.

The 2nd enciphering circuit that carries out the updating input of this encryption result value as said input in said 1st enciphering circuit while enciphering an encryption result value by said 1st enciphering circuit with said 2nd key.

An exclusion OR circuit which outputs exclusive OR of data stored in said packetand an encryption result value of said 2nd enciphering circuit.

[Claim 3]While said packet includes storing position information about a storing position of data stored in this packetThe encryption processing unit according to claim 2 having further an encryption control circuit which enables encryption by said 1st enciphering circuit and said 2nd enciphering circuit only when said data is inputted into said exclusion OR circuit based on this storing position information.

[Claim 4]The encryption processing unit according to claim 2 having detected said time information from said packetand having further an initializing means which initializes a state of said 1st enciphering circuit and said 2nd enciphering circuit.
[Claim 5]In encryption mode of processing which enciphers said data which is stored in a packet and delivered between a service provider which provides dataand a service client which receives supply of dataA key generating means in which said service provider generates the 1st key and 2nd key based on a random numberA key delivery means to deliver this the 1st key and 2nd key to said service clientThe 1st enciphering circuit that enciphers input with said 1st keyand 1st extraction means to extract time information from a header of said packetand to input this time information into said 1st enciphering circuit as an initial value of said inputWhile enciphering an encryption result value by said 1st enciphering circuit with said 2nd keyThe 2nd enciphering circuit that carries out the updating input of this encryption result value as said input in said 1st enciphering circuitThe 1st exclusion OR circuit that outputs exclusive OR of data stored in said packetand an encryption result value of said 2nd enciphering circuitHave a data delivery means to deliver said packet which was outputted from this exclusion OR circuit and stored data to said service clientand said service clientThe 3rd enciphering circuit that enciphers input with said 3rd key delivered by said said 1st key delivery means2nd extraction means to extract time information from a header of said packetand to input this time information into said 1st enciphering circuit as an initial value of said inputWhile enciphering an encryption result value by said 3rd enciphering circuit with said 2nd keyEncryption mode of processing provided with the 2nd exclusion OR circuit that outputs exclusive OR of the 4th enciphering circuit that carries out the updating input of this encryption result value as said input in said 3rd enciphering circuitdata stored in said packetand an encryption result value of said 4th enciphering circuit.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Industrial Application]In the system (digital audio interactive system) which delivers the software of image works etc. via a means of communicationthis invention relates to encryption mode of processing for enciphering this software with a specific key according to the demand from a client.
[0002]
[Description of the Prior Art]In recent yearsthe service which delivers the digital-information-ized software (it is called the following and "data" of voice datapicture image dataetc.) at each home is proposed against the background of construction of cable television and the communications system using a communications satellite. This service system is a digital audio interactive system called a video-on-demand method etc. In this digital audio interactive systemcommunication

which passed the telephone wire etc. between the purveyor of service and the user is performed. And a purveyor of service charges the usage fee of this data through a credit card company etc. at the user concernedand returns that part to a contents supplier while he delivers the data of the contents demanded at the time demanded by the user to this user.

[0003]Server/from which it becomes an infrastructure that it is important when such a digital audio interactive system spreads Network/Although a terminal is built of course by low costIf the data with which a user is provided through these is not prepared abundantlyI hear that a success does not become and there is. Namelyby including structure without a risk of suffering unexpected damagewhile a data donor can count upon the repatriation by contents offer since data and an infrastructure are the two pillars in this infrastructureIt is indispensable to fix the environment where data gathers easily. Such structure must be improved irrespective of the kinds (a broadband cable networka satellite systemmobile communicationsan optical-medium packageetc.) of media supplied which carries a data donor and a user.

[0004]Thereforedata was enciphered during delivery so that data might be monitored by the third party (third party who has not paid the usage fee of the data concerned) of a non-right and might not be unfairly used during delivery (reproduction). Drawing 6 explains encryption mode of processing in the former.

[0005]In drawing 6it is a service provider (the thing of the purveyor-of-service side system is said.). The 1st enciphering circuit [that it is below the same] 103 enciphers the data of a packet format with the key (Ks) of a pieceleads a transport layer transmission lineand is a service client (the thing of user side systems is said.). the following -- it is the same -- it delivers. The 1st decoding circuit 106 of the service client which received this enciphered data decrypts data with the key (Ks) used for encryption in the 1st enciphering circuit 103. Thusin the conventional encryption mode of processingsince only the single step which used the key (Ks) of the piece was vulnerable and the algorithm of a data encryption and decryption prevented the decipherment of a key (Ks)it needed to change the key (Ks) frequently. In order to restore promptly from the error of a channeland cuttingit was required to transmit a code synchronized signal.

[0006]In order to satisfy this conditionas shown in drawing 6the random number generator 100the master key (K1) 101and the 2nd enciphering circuit 102 were established in the service providerand the master key (K1) 104 and the 2nd decoding circuit 102 are established in the service client.

[0007]This random number generator 100 has always generated the random number series continuously. And this random number series is started by a key block unit (beam of the key defined beforehand) at intervals of several secondsand it is inputted into the 1st enciphering circuit 103 as a key (Ks) updated at intervals of several seconds. Since the key (Ks) updated in this way must be delivered by the service clientthe 2nd enciphering circuit 102The key (Ks) cut down from the random number generator 100 is enciphered with the master key (K1) 101and it delivers to a service client using a part of user quota packet (session layer) of the

transport layer. The 2nd decoding circuit 105 of the service client decrypted the enciphered key (Ks) using the master key (K1)and had inputted it into the 1st decoding circuit 106.
[0008]And whenever the 1st enciphering circuit 103 and the 1st decoding circuit 106 have an input of a new key (Ks)they reset oneselftake a synchronizationand they encipher and decrypt the data after it with a new key (Ks). The master key (K1) 101104 is a fixed key beforehand prepared for the service provider and the service client by the contentsrespectively.
[0009]Thusin the conventional data encryption mode of processingchange of a key (Ks) and code synchronous processing were performed.
[0010]
[Problem(s) to be Solved by the Invention]Howeverif it is in the above-mentioned conventional encryption mode of processingSince a new key (Ks) had to be delivered from the service provider to the service client at intervals of several secondsa lot of packets (packet for key deliveries) in addition to the packet used for original data delivery had to be transmitted. As a resultthe Information Transfer Sub-Division efficiency between service provider service clients had fallen remarkably.
[0011]The 1st SUBJECT of this invention is providing encryption mode of processing which can reduce the necessity for a frequent change of a key and can raise the Information Transfer Sub-Division efficiency between service provider service clients by strengthening an encryption algorithm.
[0012]The 2nd SUBJECT of this invention is providing encryption mode of processing which can decode difficult by using for the initial value of encryption of the relative time information on the packet header used for transmission of datadepending on generation times and using the data of the same contents as the encryption data of contents of another.
[0013]
[Means for Solving the Problem]
(The 1st mode) Chieflythe 1st mode of this invention is made in order to solve the 1st SUBJECT of the above between service provider service clients. Namelyin encryption mode of processing which enciphers said data delivered between a service provider which provides dataand a service client which receives supply of data as shown in a principle figure of drawing 1A key generating means (random number generator 110) in which said service provider generates two keys (Ks1Ks2) based on a random numberThe 1st encoding means (113) that enciphers data with two keys (Ks1Ks2) generated by this key generating means (random number generator 110)A data delivery means (transport layer transmission line) to deliver said data enciphered by this 1st encoding means (113) to said service clientThe 2nd encoding means (112) that enciphers said two keys (Ks1Ks2) with a master key (K1101) of specified substanceHave a key delivery means (session layer transmission line) to deliver said two keys (Ks1Ks2) enciphered by this 2nd encoding means (112) to said service clientand said service clientThe 1st decoding means (115) that decrypts said two enciphered keys (Ks1Ks2) which were

delivered by said key delivery means (session layer transmission line) with a master key (K1114) of said specified substanceWith said two keys (Ks1Ks2) decrypted by this 1st decoding means (115). It had the 2nd decoding means (116) that decrypts said enciphered data which was delivered by said data delivery means (transport layer transmission line) (it corresponds to Claim 1).
(The 2nd mode) The 2nd mode of this invention is made in order to solve the 1st and 2nd SUBJECT of the above by the service provider side. Namelyin encryption mode of processing in a service provider which delivers data stored in a packet to a service clientA key generating means which generates the 1st key and 2nd key based on a random numberand the 1st enciphering circuit that enciphers input with said 1st keyAn extraction means to extract time information from a header of said packetand to input this time information into said 1st enciphering circuit as an initial value of said inputWhile enciphering an encryption result value by said 1st enciphering circuit with said 2nd keyIt had the 2nd enciphering circuit that carries out the updating input of this encryption result value as said input in said 1st enciphering circuitand an exclusion OR circuit which outputs exclusive OR of data stored in said packetand an encryption result value of said 2nd enciphering circuit (it corresponds to Claim 2).
(The 3rd mode) The 3rd mode of this invention is made in order to solve the 1st and 2nd SUBJECT of the above between service provider service clients. Namelyin encryption mode of processing which enciphers said data which is stored in a packet and delivered between a service provider which provides dataand a service client which receives supply of dataA key generating means in which said service provider generates the 1st key and 2nd key based on a random numberA key delivery means to deliver this the 1st key and 2nd key to said service clientThe 1st enciphering circuit that enciphers input with said 1st keyand 1st extraction means to extract time information from a header of said packetand to input this time information into said 1st enciphering circuit as an initial value of said inputWhile enciphering an encryption result value by said 1st enciphering circuit with said 2nd keyThe 2nd enciphering circuit that carries out the updating input of this encryption result value as said input in said 1st enciphering circuitThe 1st exclusion OR circuit that outputs exclusive OR of data stored in said packetand an encryption result value of said 2nd enciphering circuitHave a data delivery means to deliver said packet which was outputted from this exclusion OR circuit and stored data to said service clientand said service clientThe 3rd enciphering circuit that enciphers input with said 1st key delivered by said said 1st key delivery means2nd extraction means to extract time information from a header of said packetand to input this time information into said 3rd enciphering circuit as an initial value of said inputWhile enciphering an encryption result value by said 3rd enciphering circuit with said 2nd keyIt had the 2nd exclusion OR circuit that outputs exclusive OR of the 4th enciphering circuit that carries out the updating input of this encryption result value as said input in said 3rd enciphering circuitdata stored in said packetand an encryption result value of said 4th enciphering circuit (it corresponds to Claim 5).

[0014]
[Function]
(Operation of Claim 1) In a service providera key generating means generates two keys based on a random number. The 1st encoding means enciphers data by performing a predetermined encryption algorithm based on two keys generated by this key generating means. The 2nd encoding means enciphers these two keys with the master key of specified substance. A data delivery means delivers the data enciphered by the 1st encoding means to a service client after more thanand a key delivery means delivers two keys enciphered by the 2nd encoding means to a service client.
[0015]On the other handin a service clientthe 1st decoding means decrypts two enciphered keys which were delivered by the key delivery means with the master key of specified substance. The 2nd decoding means decrypts the enciphered data which was delivered by the data delivery means by performing the decryption algorithm corresponding to the above-mentioned encryption algorithm based on two keys decrypted by this 1st decoding means.
[0016]Thussince it is enciphering with two keysencryption intensity becomes strong.
(Operation of Claim 2) A key generating means generates the 1st key and 2nd key based on a random number. The 1st enciphering circuit enciphers input with the 1st key. The initial value of this input is the time information extracted from the header of the packet by the extraction means. After completing encryption of an initial valuethe encryption result of the 2nd enciphering circuit serves as input.
[0017]This 2nd enciphering circuit enciphers the encryption result value by the 1st enciphering circuit with the 2nd key. An exclusion OR circuit outputs the exclusive OR of the data and the encryption result value of the 2nd enciphering circuit which were stored in the packet.
[0018]Thusin this encryption mode of processingthe 1st keythe 2nd keyand time information are used for encryption. Thereforeencryption intensity improves so much. And since time information is used and the data of the same contents can be used as encryption data with separate contents even if it fixed the 1st key and 2nd key for a whilethe decipherment by a third party becomes difficult so much.
(Operation of Claim 3) It is made for a packet to include the storing position information about the storing position of the data stored in this packetIf an encryption control circuit controls to enable encryption by the 1st enciphering circuit and 2nd enciphering circuit only when data is inputted into the exclusion OR circuit based on this storing position informationSince it can be considered except the data storage portion of a packet as as [plaintext]a service client can be decoded by reading time information from this plaintext portion.
(Operation of Claim 4) If it has further an initializing means which detects time information from a packet and initializes the state of the 1st enciphering circuit and the 2nd enciphering circuitEven if it does not transmit a synchronized signal special to the service client sidethe service client can detect this time information and can take a code synchronization autonomously.

(Operation of Claim 5) In a service providera key generating means generates the 1st key and 2nd key based on a random number. A key delivery means delivers this the 1st key and 2nd key to a service client. The 1st enciphering circuit enciphers input with the 1st key. The initial value of this input is the time information extracted from the header of the packet by the 1st extraction means. After encryption of an initial value is completedthe encryption result by the 2nd enciphering circuit serves as input. This 2nd enciphering circuit enciphers the encryption result value by the 1st enciphering circuit with the 2nd key. The 1st exclusion OR circuit outputs the exclusive OR of the data and the encryption result value of the 2nd enciphering circuit which were stored in the packet. A data delivery means delivers the packet which stored the data which did in this way and was enciphered to a service client.

[0019]On the other handin a service clientthe 3rd enciphering circuit enciphers input with the 1st key delivered by the 1st key key delivery means. The initial value of this input is the time information extracted from the header of the packet by the 2nd extraction means. After encryption of this initial value is completedthe encryption result by the 4th enciphering circuit serves as input. This 4th enciphering circuit enciphers the encryption result value by the 3rd enciphering circuit with the 2nd key. The 2nd exclusion OR circuit outputs the exclusive OR of the data and the encryption result value of the 4th enciphering circuit which were stored in the packet.

[0020]Thusin this encryption mode of processingthe 1st keythe 2nd keyand time information are used for encryption. Thereforeencryption intensity improves so much. And since time information is used and the data of the same contents can be used as encryption data with separate contents even if it fixed the 1st key and 2nd key for a whilethe decipherment by a third party becomes difficult so much.

[0021]

[Example]Hereafterone working example of this invention is described based on Drawings. This example applies encryption mode of processing by this invention to a digital audio interactive system.

<<Composition of working example>>

(Composition of SOFUTOWE) The composition of the software which circulates in the digital audio interactive system by this example is first shown in drawing 3. As shown in drawing 3one software is divided into plurality and stored in the respectively different transport packet P. This transport packet P is prescribed by MPEG.

[0022]The main header which shows the state of the data stored in each transport packet P is added to the head of each transport packet P. Varieties of informationsuch as data identification ID (ID)relative time information (PCR)and data length information (L)are included in this main header. That isdata identification ID is an identifier which shows that the data which constitutes a certain software is stored.

The same data identification ID is given to all the transport packets P which store the data which constitutes the same software.

Relative time information (PCR) is information which shows the generating time of each transport packet P.
It stops in the stage which it is updated according to the turn of the data sent one after anotherand the whole software finished sending.
Thereforethe original software is reconstructible by putting in order the data stored in the turn of this relative time information (PCR) at each transport packet P which makes data identification ID the same. The data length information (L) as storing position information is information which shows the length of the data which continues after this main header.
[0023]Data and subheader are connected with each transport packet P by turns following the main header. Each data is the picture of one frame and voice data which were compressed by the MPEG standard. Each subheader includes the data length information (L) which shows the length of the data which continues after that.
[0024](The composition of a system)next the outline of the digital audio interactive system by this example are shown in drawing 2. This digital audio interactive systemIt comprises a service client of the service provider which delivers this software according to the request from a client while storing much softwareand a large number which receive the delivered software and reproduce this. It uses for encryption of data identification ID (ID) and time information (PCR)and the composition of the digital audio interactive system by this example is the same plaintext data (the thing of unenciphered data is said.). It is below the same. Even if encipheredthe work which always completes the cryptogram of different contents is carried out. Hereafterthe detailed composition is explained for every service provider and service client.
[0025][Service provider] In a service providerthe random number generator 1 generates a random number series once in one week for every title of each software. This random number series has the length for two key block units (beam of the key for codes defined beforehand)and is inputted into 1st key buffer 162nd key buffer 17and ****** 1DES(Data Encryption Standard) 4.
[0026]The 1st key buffer 16 as a key generating means starts a top key block unit from this random number seriesand by making this into the 1st title key (Ks1)it holds this 1st title key (Ks1) until there is an input of a next random number series.
[0027]Similarlythe 2nd key buffer 17 as a key generating means starts the 2nd key block unit from this random number seriesand by making this into the 2nd title key (Ks2)it holds this 2nd title key (Ks2) until there is an input of a next random number series.
[0028]The ****** 1DES enciphering circuit 4 enciphers the random number series which consists of the 1st title key (Ks1) and the 2nd title key (Ks2) using the 1st master key (K1). The enciphered random number series is passed to the ****** 2DES enciphering circuit 5and is further enciphered using the 2nd master key (K2).
[0029]Thusthe random number series enciphered doubly is once stored in the key file 25 noting that it is a title key to a specific title. The enciphered random number series which was stored in this key file 25 will be updated by this if the

new random number series for title keys over that title is generated in one week.
[0030]On the other handto compensate for a random number series occurring from the random number generator 1it is enciphered by a title key (Ks1Ks2) new once per weekand the software of each title is stored in the cumulative file 9. Namelythe software of a certain title stored in the cumulative file 9 is updated once per week. In order to perform this updatingthe transport packet P group which has same discernment ID (ID) that stores the data of a plaintext receives processing in order of relative time information (PCR).
[0031]From the main header of each transport packet Pdiscernment ID (ID) and relative time information (PCR) are extractedand it is inputted into the 1st DES enciphering circuit 6 for titlesand the DES set / reset circuit 22 (equivalent to an extraction means). Data length information (L) is extracted from a main headerandsimultaneously with itit is inputted into the data strobe signal detector 21. Also from the subheader of each transport packet Pdata length information (L) is extracted and it is inputted into the data strobe signal detector (ST) 21. Thusthe transport packet P from which the variety of information was extracted is inputted into one input terminal of exclusion OR circuit 8 sequentially from the main header side.
[0032]The DES set / reset circuit 22 as an initializing meansIf discernment ID (ID) and relative time information (PCR) are detected from the inputted dataIt judges that the processing to the new transport packet P was startedthe 1st DES enciphering circuit 6 for titles and the 2nd DES enciphering circuit 7 for titles are resetand those internal states are made into an initial state. As a resultin this examplea code synchronization will be taken in the head of each transport packet P. That iswhenever the new transport packet P is inputted and discernment ID (ID) and relative time information (PCR) are inputtedthe DES enciphering circuits 6 and 7 for both titles will be initializedand encryption will be resumed by making this discernment ID (ID) and relative time information (PCR) into an initial value.
[0033]The 1st DES enciphering circuit 6 for titles as the 1st enciphering circuit enciphers input using the 1st title key (Ks1) currently held at the 1st key buffer 16. In the initial state after resetalthough the 1st DES enciphering circuit 6 for titles enciphers discernment ID (ID) and relative time information (PCR) as an initial valueit enciphers the data which returns from the 2nd DES enciphering circuit 6 for titles until it is reset again henceforth.
[0034]The 2nd DES enciphering circuit 7 for titles as the 2nd enciphering circuit enciphers further the input from the 1st DES enciphering circuit 6 for titles using the 2nd title key (Ks2) currently held at the 2nd key buffer 17. As a resultdisturbance nature is improved further. The output of the 2nd DES enciphering circuit 7 for titles is inputted into the input terminal of another side of exclusion OR circuit 8 while it returns to the input edge of the 1st DES enciphering circuit 6 for titles. This return is repeated until each DES enciphering circuits 6 and 7 for titles are reset by a DES set / reset circuit 22.
[0035]The data strobe signal detector (ST) 21 as an encryption control circuitIn order to carry out encryption processing only of the data in a transport

packetdata length information (L) is extracted from the main header of each transport packet PThe control signal which starts / stops encryption of each DES enciphering circuits 6 and 7 for titles based on this data length information (L)i.e.a data strobeis outputted. Namelythis data strobe is the timing as which the head portion of each data in each transport packet P was inputted into exclusion OR circuit 8Encryption by each DES enciphering circuits 6 and 7 for titles is made to startit is the timing which passed exclusion OR circuit 8and the terminal part of each data is a pulse which stops encryption by each DES enciphering circuits 6 and 7 for titles. If encryption is stopped by the data strobethe 2nd DES enciphering circuit 7 for titles will continue outputting "0."

[0036]Exclusion OR circuit 8 outputs the exclusive OR of the contents of the transport packet P of a plaintextand the encryption data from the 2nd DES enciphering circuit 7 for titles. That issince the DES enciphering circuits 6 and 7 for both titles are not enciphering when the portion of the header (a main header and subheader) in each transport packet P is inputtedexclusion OR circuit 8 outputs the contents of this header with a plaintext. Since the DES enciphering circuits 6 and 7 for both titles are enciphering when the portion of the data in each transport packet P is inputtedthe logical value of input data is reversed according to the encipherment information from the 2nd DES enciphering circuit 7 for titlesand it outputs.

[0037]Thusthe encryption data which attached the header (a main headersubheader) of the plaintext is madeand it is accumulated in the cumulative file 9. If the transport packet P provided with the following relative time information (PCR) which has the same discernment ID becomes a processing objectThe DES enciphering circuits 6 and 7 for both titles are resetand encryption new as an initial value is performed in discernment ID and relative time information (PCR) of the transport packet P. Thusall the encryption data which constitutes a certain title is stored in the cumulative file 9. When the encryption data about the software of the same title is already stored into the cumulative file 9 at this timeold encryption data is updated with new encryption data.

[0038]Thusthe encryption data (transport packet P) of each title accumulated in the cumulative file 9According to the demand from which service clientit is read from the cumulative file 9 in order of relative time information (PCR)and is delivered by the service client of a requiring agency via the transport layer transmission line as a data delivery means. At this timethe enciphered random number series corresponding to the title of the encryption data (transport packet P) deliveredIt is read from the key file 25 and delivered by the service client using a part of user quota packet (session layer transmission line as a key delivery means) of the transport layer.

[0039][Service client] The enciphered random number series received via the session layer transmission line in the service client is inputted into the ****** 1DES decoding circuit 12. This ****** 1DES decoding circuit 12 decrypts using the 1st master key (K1) 10 by performing an algorithm completely contrary to the ****** 1DES enciphering circuit 4. This 1st master key (K1) 10 is a fixed key of

the completely same contents as the thing by the side of a service provider.
[0040]The output of the ****** 1DES decoding circuit 12 is inputted into the ****** 2DES decoding circuit 13. This ****** 2DES decoding circuit 13 decrypts using the 2nd master key (K2) 11 by performing an algorithm completely contrary to the ****** 2DES enciphering circuit 5. This 2nd master key (K2) 11 is a fixed key of the completely same contents as the thing by the side of a service provider.
[0041]The output of the ****** 2DES decoding circuit 13 which passed these two steps of decryption processes becomes the random number series itself generated from the random number generator 1. This random number series is inputted into the 1st key buffer 18 and the 2nd buffer 19respectively.
[0042]The 1st key buffer 18 starts a top key block unit from this random number seriesand by making this into the 1st title key (Ks1)it holds this 1st title key (Ks1) until there is an input of a next random number series.
[0043]Similarlythe 2nd key buffer 19 starts the 2nd key block unit from this random number seriesand by making this into the 2nd title key (Ks2)it holds this 2nd title key (Ks2) until there is an input of a next random number series.
[0044]On the other handthe transport packet P received via the transport layer is inputted into exclusion OR circuit 20 in order. Before being inputted into this exclusion OR circuit 20from the main header of each transport packet P. Beforehanddiscernment ID (ID) and relative time information (PCR) are extractedand it is inputted into the 1st DES decoding circuit 14 for titlesand the DES set / reset circuit 24 (equivalent to the 2nd extraction means). Data length information (L) is extracted from a main headerandsimultaneously with itit is inputted into the data strobe signal detector 23. Also from the subheader of each transport packet Pdata length information (L) is extracted and it is inputted into the data strobe signal detector (ST) 23.
[0045]If discernment ID (ID) and relative time information (PCR) are detected from the inputted dataa DES set / reset circuit 24It judges that the processing to a new transport packet was startedthe 1st DES enciphering circuit 14 for titles and the 2nd DES enciphering circuit 15 for titles are resetand those internal states are made into an initial state. As mentioned abovein this examplea code synchronization is taken in the head of each transport packet. Thereforeif the head of the following transport packet is detected and the DES enciphering circuits 14 and 15 for both titles are reset in a service client when there are an error of a channel and cuttingit can return to a synchronous state autonomously.
[0046]The 1st DES enciphering circuit 14 for titles as the 3rd enciphering circuit enciphers input data using the 1st title key (Ks1) currently held at the 1st key buffer 18 with the same algorithm as the 1st DES enciphering circuit 6 for titles of a service provider. In the initial state after resetalthough the 1st DES enciphering circuit 14 for titles enciphers discernment ID (ID) and relative time information (PCR) as an initial valueit enciphers the data which returns from the 2nd DES enciphering circuit 15 for titles until it is reset again henceforth.
[0047]The 2nd DES enciphering circuit 15 for titles as the 4th enciphering circuitThe input data from the 1st DES enciphering circuit 14 for titles is further

enciphered using the 2nd title key (Ks2) currently held at the 2nd key buffer 19 with the same algorithm as the 2nd DES enciphering circuit 7 for titles of a service provider. The output of the 2nd DES enciphering circuit 15 for titles is inputted into the input terminal of another side of exclusion OR circuit 20 while it returns to the input edge of the 1st DES enciphering circuit 14 for titles. This return is repeated until each DES enciphering circuits 14 and 15 for titles are reset by a DES set / reset circuit 24.

[0048]The data strobe signal detector (ST) 23In order to carry out encryption processing only of the data in the transport packet Pdata length information (L) is extracted from the main header of each transport packet PThe control signal which starts / stops encryption of each DES enciphering circuits 14 and 15 for titles based on this data length information (L)i.e.a data strobeis outputted. That isthis data strobe is a pulse to which encryption by each DES enciphering circuits 14 and 15 for titles is made to carry outonly when the enciphered data part in each transport packet P is inputted into exclusion OR circuit 20. If encryption is stopped by the data strobethe 2nd DES enciphering circuit 15 for titles will continue outputting "0."

[0049]As mentioned abovethe circuit after the 1st key buffer 18 in a service client and the 2nd key buffer 19 is completely the same as the thing of a service provider. Thereforethe encipherment information from the 2nd DES enciphering circuit 15 for titles inputted into exclusion OR circuit 20 is completely the same as the encipherment information from the 2nd DES enciphering circuit 7 for titles inputted into exclusion OR circuit 8 in a service provider. Thereforeexclusion OR circuit 20 outputs the contents of this header with a plaintextwhen the portion of the header (a main header and subheader) in each transport packet P is inputted. When the portion of the data in each transport packet P is inputteda logical value is reversed according to the encipherment information from the 2nd DES enciphering circuit 15 for titlesand it outputs. As for this encryption datathat logical value is reversed from the first by encryption. Thereforeby re-reversal in exclusion OR circuit 20since the logical value returns to the original statethe data of the plaintext before encryption can be restored.

<<Operation of working example>> As mentioned abovethe DES enciphering circuit for titles is doubled in both the service provider and the service client side by this example. Thereforesince the encryption algorithm was strengthenedthe third party (a user is included) decoded two title keys based on the transport packetand it became very difficult to decrypt encryption data. Drawing 4 and drawing 5 are based and this is explained.

[0050]Nowsupposing you input a value "I" in the 1st DES enciphering circuit 14 for titlessuppose that the value "O" was outputted to the outgoing end of the 2nd DES enciphering circuit 15 for titles. In this casein order to decode title key Ks1 currently held at the 1st key buffer 18 and the 2nd key buffer 19and Ks2As shown in drawing 4a known value "I" is continuously inputted into the 1st DES enciphering circuit 14 for titlesit changes into original title key Ks1and various values (presumed key: Ks1m) and the output value "C" of the 1st DES enciphering

circuit 14 for titles to these are measured. And the relation of the presumed key (Ks1m) and output value "C" which were measured is summarized in Table 30as shown in drawing 5.

[0051]Similarlyvarious presumed keys (Ks2m) are inputted into the 2nd DES enciphering circuit 15 for titlesand the output of this 2nd DES enciphering circuit 15 for titles measures the input value "C" which maintains a known value "O." And the relation of the presumed key (Ks2m) and input value "C" which were measured is summarized in Table 32as shown in drawing 5.

[0052]Thusif the same mean value "C1k" as both tables appears when the two created tables 30 and 32 are contrastedthe presumed key "Ks1" corresponding to this value "C1k" and "Ks2" can decode that it is 1st title key Ks1 and 2nd title key Ks2respectively.

[0053]such a method (**********: middle match attack) of decoding a key -- howevermany processing time and memory resources are needed. For examplethe number of times of procedure of a 2^{55} time is requiredand in order to create the above-mentioned tablethe memory of a 2^{56} word (1 word 64 bits) is needed in the case of a 70-bit plaintext and a cryptogram pair. Thereforeif the DES circuit of 16 steps of insides is made into two stepsa decipherment will become difficult as a matter of fact.

[0054]Since what is necessary is just to discover the presumed key which outputs a known output value to a known input value if ********** when a DES circuit is made into one step for comparison is explainedthe time and effort of processing passes substantially. Since it can succeed only by the number of times of procedure of a 2^{55} time in the case of a 70-bit plaintext and a cryptogram pair if the above-mentioned example is metit will be decipherable with the 100000-dol device of Wiener in about 35 hours. As a resultrenewal of a title key can be made into about 1 time per week in this example. Thereforethe problem consumed for title key delivery of communication channel capacity can be solvedand the Information Transfer Sub-Division efficiency between service provider service clients can be raised.

[0055]In order to make such the number of times of title key delivery decrease sharplythe necessity of separating a code synchronization from renewal of a keyand performing it arises secondarily. In this examplesince discernment ID (ID) and relative time information (PCR) which are stored in the header of the transport packet for delivering data are performing the code synchronizationeven if it makes the number of times of title key delivery decrease sharplya code synchronization can be performed. And this relative time information (PCR) takes a value which is therefore different in the generating time of a transport packet. Thereforeeven when the plaintext data of the completely same contents is encipheredthe data which enciphered this plaintext data turns into completely different data.

[0056]

[Effect of the Invention]A frequent change of a key decreasesand since a code synchronized signal utilizes the time information with which the system is equipped

beforehandit becomes unnecessary to sacrifice a part of user packet for it for strengthening of a cryptographic algorithmand a code synchronization according to encryption mode of processing of this invention constituted as mentioned above.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]The principle figure showing the principle of this invention
[Drawing 2]The schematic diagram of the digital audio interactive system with which encryption mode of processing by one working example of this invention was applied
[Drawing 3]The explanatory view showing the structure of each transport packet where the data which constitutes one software was stored
[Drawing 4]The explanatory view of the ********** method by middle match attack
[Drawing 5]The explanatory view of the ********** method by middle match attack
[Drawing 6]The approximate account figure of the conventional encryption mode of processing
[Description of Notations]
1 Random number generator
6 The 1st DES enciphering circuit for titles
7 The 2nd DES enciphering circuit for titles
8 Exclusion OR circuit
14 The 1st DES enciphering circuit for titles
15 The 2nd DES enciphering circuit for titles
16 The 1st title key buffer
17 The 2nd title key buffer
18 The 1st title key buffer
19 The 2nd title key buffer
20 Exclusion OR circuit
21 Data strobe signal detector (ST)
22 A DES set / reset circuit
23 Data strobe signal detector (ST)
24 A DES set / reset circuit
